Table of Contents

2 Functional Capabilities

2.1 Scope

This section contains standards detailing the functional capabilities required of a voting system. This section sets out precisely what it is that a voting system is required to do. In addition, this section sets forth the minimum actions a voting system must be able to perform to be eligible for qualification.
For organizational purposes, functional capabilities are categorized by the phase of election activity in which they are required:
Overall Capabilities: These functional capabilities apply throughout the election process. They include security, accuracy, integrity, system auditability, election management system, vote tabulation, ballot counters, telecommunications, and data retention.

Pre-voting Capabilities: These functional capabilities are used to prepare the voting system for voting. They include ballot preparation, the preparation of election-specific software (including firmware), the production of ballots or ballot pages, the installation of ballots and ballot counting software (including firmware), and system and equipment tests.

Voting Capabilities: These functional capabilities include all operations conducted at the polling place by voters and officials including the generation of status messages.

Post-voting Capabilities: These functional capabilities apply after all votes have been cast. They include closing the polling place; obtaining reports by voting machine, polling place, and precinct; obtaining consolidated reports; and obtaining reports of audit trails.

Maintenance, Transportation and Storage Capabilities: These capabilities are necessary to maintain, transport, and store voting system equipment.

In recognition of the diversity of voting systems, the Standards apply specific requirements to specific technologies. Some of the Standards apply only if the system incorporates certain optional functions (for example, voting systems employing telecommunications to transmit voting data). For each functional capability, common standards are specified. Where necessary, common standards are followed by standards applicable to specific technologies (i.e., paper-based or DRE) or intended use (i.e., central or precinct count).

2.2 Overall System Capabilities

This section defines required functional capabilities that are system-wide in nature and not unique to pre-voting, voting, and post-voting operations. All voting systems shall provide the following functional capabilities:
Security;
Accuracy;
Error recovery;
Integrity;
System auditability;
Election management system;

Accessibility:
Vote tabulating;
Ballot counters; and
Data Retention.
Voting systems may also include telecommunications components. Technical standards for these capabilities are described in Sections 3 through 6 of the Standards.

2.2.1 Security

System security is achieved through a combination of technical capabilities and sound administrative practices. To ensure security, all systems shall:
Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability.

Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.

Use the system's control logic to prevent a system function from executing if any preconditions to the function have not been met.

Provide safeguards to protect against tampering during system repair, or interventions in system operations, in response to system failure.

Provide security provisions that are compatible with the procedures and administrative tasks involved in equipment preparation, testing, and operation.

If access to a system function is to be restricted or controlled, the system shall incorporate a means of implementing this capability.

Provide documentation of mandatory administrative procedures for effective system security.

2.2.2 Accuracy

Memory hardware, such as semiconductor devices and magnetic storage media, must be accurate. The design of equipment in all voting systems shall provide for the highest possible levels of protection against mechanical, thermal, and electromagnetic stresses that impact system accuracy. Section 3 provides additional information on susceptibility requirements.

2.2.2.1 **Common Standards**

To ensure vote accuracy, all systems shall:
Record the election contests, candidates, and issues exactly as defined by election officials;

Record the appropriate options for casting and recording votes;

Record each vote precisely as indicated by the voter and be able to produce an accurate report of all votes cast;

Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the system has been designed for accuracy; and

Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected.

2.2.2.2 **DRE System Standards**

As an additional means of ensuring accuracy in DRE systems, voting devices shall record and retain redundant copies of the original ballot image. A ballot image is an electronic record of all votes cast by the voter, including undervotes.

2.2.3 Error Recovery

To recover from a non-catastrophic failure of a device, or from any error or malfunction that is within the operator's ability to correct, the system shall provide the following capabilities:
Restoration of the device to the operating condition existing immediately prior to the error or failure, without loss or corruption of voting data previously stored in the device;

Resumption of normal operation following the correction of a failure in a memory component, or in a data processing component, including the central processing unit; and

Recovery from any other external condition that causes equipment to become inoperable, provided that catastrophic electrical or mechanical damage due to external phenomena has not occurred.

2.2.4 Integrity

Integrity measures ensure the physical stability and function of the vote recording and counting processes.

2.2.4.1 **Common Standards**

To ensure system integrity, all systems shall:
Protect, by a means compatible with these Standards, against a single point of failure that would prevent further voting at the polling place;

Protect against the interruption of electronic power;

Protect against generated or induced electromagnetic radiation;

Protect against ambient temperature and humidity fluctuations;

Protect against the failure of any data input or storage device;

Protect against any attempt at improper data entry or retrieval;

Record and report the date and time of normal and abnormal events;

Maintain a permanent record of all original audit data that cannot be modified or overridden but may be augmented by designated authorized officials in order to adjust for errors or omissions (e.g. during the canvassing process.)

Detect and record every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator; and

Include built-in measurement, self-test, and diagnostic software and hardware for detecting and reporting the system's status and degree of operability.

2.2.4.2 **DRE Systems Standards**

In addition to the common standards, DRE systems shall:
Maintain a record of each ballot cast using a process and storage location that differs from the main vote detection, interpretation, processing, and reporting path; and

Provide a capability to retrieve ballot images in a form readable by humans.

2.2.5 System Audit

This section describes the context and purpose of voting system audits and sets forth specific functional requirements. Additional technical audit requirements are set forth in Section 4.

2.2.5.1 **System Audit Purpose and Context**

Election audit trails provide the supporting documentation for verifying the correctness of reported election results. They present a concrete, indestructible archival record of all system activity related to the vote tally, and are essential for public confidence in the accuracy of the tally, for recounts, and for evidence in the event of criminal or civil litigation.

The following audit trail requirements are based on the premise that system-generated creation and maintenance of audit records reduces the chance of error associated with manually generated audit records. Because most audit capability is automatic, the system operator has less information to track and record, and is less likely to make mistakes or omissions.

The sections that follow present operational requirements critical to acceptable performance and reconstruction of an election. Requirements for the content of audit records are described in Section 4 of the Standards.

The requirements for all system types, both precinct and central count, are described in generic language. Because the actual implementation of specific characteristics may vary from system to system, it is the responsibility of the vendor to describe each system's characteristics in sufficient detail that ITAs and system users can evaluate the adequacy of the system's audit trail. This description shall be incorporated in the System Operating Manual, which is part of the Technical Data Package (TDP).

Documentation of items such as paper ballots delivered and collected, administrative procedures for system security, and maintenance performed on voting equipment are also part of the election audit trail, but are not covered in these technical standards. Future volumes of the Standards will address these and other system operations practices. In the interim, useful guidance is provided by the Innovations in *Election Administration #10, Ballot Security and Accountability*, available from the FEC's Office of Election Administration.

2.2.5.2 **Operational Requirements**

Audit records shall be prepared for all phases of elections operations performed using devices controlled by the jurisdiction or its contractors. These records rely upon automated audit data acquisition and machine-generated reports, with manual input of some information. These records shall address the ballot preparation and election definition phase, system readiness tests, and voting and ballot-counting operations. The software shall activate the logging and reporting of audit data as described in the following sections.

2.2.5.2.1 Time, Sequence, and Preservation of Audit Records

The timing and sequence of audit record entries is as important as the data contained in the record. All voting systems shall meet the following requirements for time, sequence and preservation of audit records:

Except where noted, systems shall provide the capability to create and maintain a real-time audit record. This capability records and provides the operator or precinct official with continuous updates on machine status. This information allows effective operator identification of an error condition requiring intervention, and contributes to the reconstruction of election-related events necessary for recounts or litigation.

All systems shall include a real-time clock as part of the system's hardware. The system shall maintain an absolute record of the time and date or a record relative to some event whose time and data are known and recorded.

All audit record entries shall include the time-and-date stamp.

The audit record shall be active whenever the system is in an operating mode. This record shall be available at all times, though it need not be continually visible.

The generation of audit record entries shall not be terminated or altered by program control, or by the intervention of any person. The physical security and integrity of the record shall be maintained at all times.

Once the system has been activated for any function, the system shall preserve the contents of the audit record during any interruption of power to the system until processing and data reporting have been completed.

The system shall be capable of printing a copy of the audit record. A separate printer is not required for the audit record, and the record may be produced on the standard system printer if all the following conditions are met:
The generation of audit trail records does not interfere with the production of output reports;

The entries can be identified so as to facilitate their recognition, segregation, and retention; and

The audit record entries are kept physically secure.

2.2.5.2.2 Error Messages

All voting systems shall meet the following requirements for error messages:
The system shall generate, store, and report to the user all error messages as they occur;

All error messages requiring intervention by an operator or precinct official shall be displayed or printed unambiguously in easily understood language text, or by means of other suitable visual indicators;

When the system uses numerical error codes for trained technician maintenance or repair, the text corresponding to the code shall be self-contained, or affixed inside the unit device. This is intended to reduce inappropriate reactions to error conditions, and to allow for ready and effective problem correction;

All error messages for which correction impacts vote recording or vote processing shall be written in a manner that is understandable to an election official who possesses training on system use and operation, but does not possess technical training on system servicing and repair;

The message cue for all systems shall clearly state the action to be performed in the event that voter or operator response is required;

System design shall ensure that erroneous responses will not lead to irreversible error; and

Nested error conditions shall be corrected in a controlled sequence such that system status shall be restored to the initial state existing before the first error occurred.

2.2.5.2.3 Status Messages

The Standards provide latitude in software design so that vendors can consider various user processing and reporting needs. The jurisdiction may require some status and information messages to be displayed and reported in real-time. Messages that do not require operator intervention may be stored in memory to be recovered after ballot processing has been completed.

The system shall display and report critical status messages using unambiguous indicators or English language text. The system need not display non-critical status messages at the time of occurrence. Systems may display non-critical status messages (i.e., those that do not require operator intervention) by means of numerical codes for subsequent interpretation and reporting as unambiguous text.

Systems shall provide a capability for the status messages to become part of the real-time audit record. The system shall provide a capability for a jurisdiction to designate critical status messages.

2.2.5.3 **COTS General Purpose Computer System Requirements**

Further requirements must be applied to COTS operating systems to ensure completeness and integrity of audit data for election software. These operating systems are capable of executing multiple application programs simultaneously. These systems include both servers and workstations (or “PCs”), including the many varieties of UNIX and Linux, and those offered by Microsoft and Apple. Election software running on these COTS systems is vulnerable to unintended effects from other user sessions, applications, and utilities, executing on the same platform at the same time as the election software. “Simultaneous processes” of concern include unauthorized network connections, unplanned user logins, and unintended execution or termination of operating system processes. An unauthorized network connection or unplanned user login can host unintended processes and user actions, such as the termination of operating system audit, the termination of election software processes, or the deletion of election software audit and logging data. The execution of an operating system process could be a full system scan at a time when that process would adversely affect the election software processes. Operating system processes improperly terminated could be system audit or malicious code detection.

To counter these vulnerabilities, three operating system protections are required on all such systems on which election software is hosted. First, authentication shall be

configured on the local terminal (display screen and keyboard) and on all external connection devices ("network cards" and "ports"). This ensures that only authorized and identified users affect the system while election software is running.
Second, operating system audit shall be enabled for all session openings and closings, for all connection openings and closings, for all process executions and terminations, and for the alteration or deletion of any memory or file object. This ensures the accuracy and completeness of election data stored on the system. It also ensures the existence of an audit record of any person or process altering or deleting system data or election data.
Third, the system shall be configured to execute only intended and necessary processes during the execution of election software. The system shall also be configured to halt election software processes upon the termination of any critical system process (such as system audit) during the execution of election software.

2.2.6 Election Management System

The Election Management System (EMS) is used to prepare ballots and programs for use in casting and counting votes, and to consolidate, report, and display election results. An EMS shall generate and maintain a database, or one or more interactive databases, that enables election officials or their designees to perform the following functions:
Define political subdivision boundaries and multiple election districts as indicated in the system documentation;

Identify contests, candidates, and issues

Define ballot formats and appropriate voting options;

Generate ballots and election-specific programs for vote recording and vote counting equipment;

Install ballots and election-specific programs;

Test that ballots and programs have been properly prepared and installed;

Accumulate vote totals at multiple reporting levels as indicated in the system documentation;

Generate the post-voting reports required by Section 2.5; and

Process and produce audit reports of the data indicated in Section 4.5.